UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/795,929	03/08/2004	Leo M. Pedlow JR.	SNY-T5718.02	1819

24337   7590   09/20/2007

MILLER PATENT SERVICES
2500 DOCKERY LANE
RALEIGH, NC 27606

EXAMINER
JOHNSON, CARLTON

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
09/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*08 March 2004*</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-57* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>*08 March 2004*</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *3-8-2004*.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   This action is responding to application papers filed on **3-8-2004**.

2.   Claims **1 - 57** are pending. Claims **1, 9, 16, 23, 29, 35, 41, 47, 52** are

independent.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art
> are such that the subject matter as a whole would have been obvious at the time the invention was made
> to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

4.   Claim **1 - 40** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Addington et al. (US Patent No. **7,194,756**) in view of **Bestler et al.** (US Patent No.

4,995,080).

Regarding Claim 1, Addington discloses an apparatus for default encryption of content

for distribution, comprising:

  a) a conditional access system; (see Addington Figure 8, number 27 ; col. 12 , lines

     22-29; col. 15, lines 14-22: access system for management of cable functions,

     conditional access (CA) module (conditional access system))

  b) a conditional access management system that communicates with and manages

     the conditional access system; (see Addington Figure 8, number 1b ; col. 12 ,

lines 2-5; col. 15, lines 14-22: conditional access system (conditional access

management system)) and

Addington discloses wherein a memory storing default encryption information for use

by the conditional access system to encrypt certain content. (see Addington col. 12,

lines 2-5; col. 45, lines 39-41: memory for encryption keys storage) Addington does

not specifically disclose whereby encrypt certain content upon a communication

failure between the conditional access system and the conditional access

management system.

However, Bestler discloses wherein:

c) default encryption information for use by the conditional access system to encrypt

   certain content upon a communication failure between the conditional access

   system and the conditional access management system.   (see Bestler col. 3,

   lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption

   information (default) utilized for decryption during communications failure)

   It would have been obvious to one of ordinary skill in the art to modify

Addington as taught by Bestler to enable the capability for usage by the conditional

access system to encrypt certain content upon a communication failure between the

conditional access system and the conditional access management system.   One of

ordinary skill in the art would have been motivated to employ the teachings of

Bestler in order to enable the capability for a novel and improved method to operate

a pay television (cable system) and permit a subscriber to self-authorize his

equipment to unscramble pay per view programs. (see Bestler col. 1, lines 28-32: "

... This invention relates generally to a novel method of operating a pay television

system and particularly to an improved method of operating a pay television system

that permits a subscriber to self-authorize his terminal to unscramble special pay per

view television programs. ... ")

Regarding Claims 2, 10, 18, 25, 31, 37, Addington discloses the apparatus of claims 1,

9, 16, 23, 29, 35, wherein the default encryption information comprises default

encryption keys. (see Addington col. 43, lines 2-7; col. 49, lines 58-62; col. 53, lines 39-

45: encryption information (keys) for content encryption)

Regarding Claims 3, 11, 19, 26, 32, 38, Addington discloses the apparatus of claims 2,

10, 18, 25, 31, 37, wherein the default encryption keys are unique for each of a plurality

of channels. (see Addington col. 2, lines 60-64: encryption key unique for each channel)

Regarding Claim 4, Addington discloses the apparatus of claim 1, further comprising a

control computer that initializes the configuration memory with the default encryption

information. (see Addington col. 12, lines 2-5; col. 43, lines 15-30; col. 45, lines 25-28;

col. 45, lines 39-41: memory, setup configuration information (encryption information))

Regarding Claims 5, 12, 20, 27, 33, 39, Addington discloses the apparatus of claims 1,

9, 16, 23, 29, 35, wherein the configuration memory comprises a non-volatile memory.

(see Addington col. 12, lines 2-5: non-volatile memory utilized for operational

(configuration) information)

Regarding Claims 6, 13, Addington discloses the apparatus of claims 1, 9, wherein the

content is encrypted with the encryption information. (see Addington col. 12, lines 2-5;

col. 43, lines 15-21; col. 45, lines 25-28: pre-setup configuration information (encryption

keys)) Addington does not specifically disclose whereby if a communication failure

occurs between the conditional access management system and the conditional access

system. However, Bestler discloses wherein, content is encrypted with the default

encryption information if a communication failure occurs between the conditional access

management system and the conditional access system. (see Bestler col. 3, lines 1-6;

col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information (default)

utilized for decryption during communications failure)

It would have been obvious to one of ordinary skill in the art to modify Addington as

taught by Bestler to enable the capability for encryption with the default encryption

information if a communication failure occurs. One of ordinary skill in the art would

have been motivated to employ the teachings of Bestler in order to enable the capability

for a novel and improved method to operate a pay television (cable system) and permit

a subscriber to self-authorize his equipment to unscramble pay per view programs.

(see Bestler col. 1, lines 28-32)

Regarding Claims 7, 14, Addington discloses the apparatus of claims 1, 9, wherein the

content is encrypted with the default encryption information. (see Addington col. 42, lines 52-60: encryption of content utilizing encryption keys) Addington does not specifically disclose whereby if communication cannot be established between the conditional access management system and the conditional access system. However, Bestler discloses wherein content is encrypted with the default encryption information, if communication cannot be established between the conditional access management system and the conditional access system. (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information (default) utilized for decryption during communications failure)

It would have been obvious to one of ordinary skill in the art to modify Addington as taught by Bestler to enable the capability for encryption with the default encryption information if communication cannot be established. One of ordinary skill in the art would have been motivated to employ the teachings of Bestler in order to enable the capability for a novel and improved method to operate a pay television (cable system) and permit a subscriber to self-authorize his equipment to unscramble pay per view programs. (see Bestler col. 1, lines 28-32)

Regarding Claims 8, 15, 21, Addington discloses the apparatus according to claims 1, 9, 16, wherein the conditional access system provides selective encryption of the content. (see Addington col. 42, lines 52-60: selective encryption (encryption of partial content))

Regarding Claim 9, Addington discloses an apparatus for default encryption,

comprising:

    a) a conditional access system; (see Addington Figure 8, number 27 ; col. 12 , lines

        22-29; col. 15, lines 14-22: access system for management of cable functions,

        conditional access (CA) module (conditional access system))

    b) means for distributing content in the conditional access system; (see Addington

        col. 13, line 46 - col. 14, line 7: content (encrypted) distributed over

        communications medium; col. 11, lines 57-61; col. 12, lines 2-5: software

        implementation, means)

    c) means for managing the conditional access system; (see Addington Figure 8,

        number 1b ; col. 12 , lines 2-5; col. 15, lines 14-22: conditional access system

        (conditional access management system); col. 11, lines 57-61; col. 12, lines 2-5:

        software implementation, means)

    d) means for communicating between the managing means and the distributing

        means; (see Addington col. 43, lines 15-30: command processing, conditional

        access system)

    f) means for configuring the storing means with the default encryption information.

        (see Addington col. 43, lines 15-30; col. 45, lines 25-28:configure encryption

        information; col. 11, lines 57-61; col. 12, lines 2-5: software implementation,

        means)

Addington discloses wherein means for storing default encryption information for the

conditional access system for use by the conditional access system to encrypt

certain content. (see Addington col. 12, lines 2-5; col. 45, lines 39-41: storage

configuration (encryption) information)   Addington does not specifically discloses

whereby a communication failure between the conditional access system and the

conditional access management system.

However, Bestler discloses wherein:

e) a communication failure between the conditional access system and the

   conditional access management system; (see Bestler col. 3, lines 1-6; col. 5,

   lines 19-22; col. 5, lines 37-39; col. 5, lines 60-63: encryption information

   (default) utilized for decryption during communications failure)

   It would have been obvious to one of ordinary skill in the art to modify

Addington as taught by Bestler to enable the capability for encryption with the default

encryption information if communication cannot be established.   One of ordinary

skill in the art would have been motivated to employ the teachings of Bestler in order

to enable the capability for a novel and improved method to operate a pay television

(cable system) and permit a subscriber to self-authorize his equipment to

unscramble pay per view programs.   (see Bestler col. 1, lines 28-32)

Regarding Claim 16, Addington discloses a method of default encryption of content for

distribution, comprising:

a) initializing a default configuration memory with default encryption information;

   (see Addington col. 12, lines 2-5: memory; col. 45, lines 39-41: initialize memory;

col. 49, lines 58-62; col. 53, lines 39-45: transfer (initialize) with configuration

(encryption) information)

b) communicating with a conditional access management system to retrieve active

encryption information for a conditional access system; (see Addington col. 43,

lines 2-7; col. 49, lines 58-62; col. 53, lines 39-45: receive (transfer) encryption

keys, normal operation)

c) encrypting content for distribution with the active encryption information;

distributing the content encrypted with active encryption information; (see

Addington col. 42, lines 52-60: content encrypted with encryption keys)

e) distributing the content encrypted with the default encryption information. (see

Addington col. 13, line 46 - col. 14, line 7: content (encrypted) distributed over

communications medium)

f) encrypting the content with the default encryption information; (see Addington

col. 42, lines 52-60: encrypt content utilizing encryption keys)

Addington does not specifically disclose if a communication failure occurs

between the conditional access management system and the conditional access

system.

However, Bestler discloses wherein:

if a communication failure occurs between the conditional access management

system and the conditional access system:

d) reading the default encryption information from the default configuration

memory; (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39;

col. 5, lines 60-63: encryption information (default) utilized for decryption

during communications failure)

It would have been obvious to one of ordinary skill in the art to modify

Addington as taught by Bestler to enable the capability for reading the default

encryption information if communication cannot be established.   One of ordinary

skill in the art would have been motivated to employ the teachings of Bestler in

order to enable the capability for a novel and improved method to operate a pay

television (cable system) and permit a subscriber to self-authorize his equipment

to unscramble pay per view programs.   (see Bestler col. 1, lines 28-32)

Regarding Claim 17, Addington discloses the method of claim 16, further comprising:

if communication is restored between the conditional access management system

and the conditional access system:

a) communicating with the conditional access management system to retrieve

active encryption information for the conditional access system; (see Addington

col. 49, lines 58-62; col. 53, lines 39-45: retrieve configuration (encryption)

information, normal operation)

b) encrypting the content for distribution with the active encryption information; (see

Addington col. 42, lines 52-60: encrypt content utilizing encryption information)

and

   c) distributing the content encrypted with active encryption information. (see

       Addington col. 13, line 46 - col. 14, line 7: content (encrypted) distributed over

       communications medium)

Regarding Claims 22, 28, 34, 40, Addington discloses a computer readable medium

storing instructions which, when executed on a programmed processor, carry out the

process according to claims 16, 23, 29, 35. (see Addington col. 11, lines 57-61; col. 12,

lines 2-5: software implementation)

Regarding Claim 23, Addington discloses a method of default encryption of content for

distribution, comprising:

   a) initializing a default configuration memory with default encryption information;

       (see Addington col. 12, lines 2-5: memory; col. 45, lines 39-41: initialize memory;

       col. 49, lines 58-62; col. 53, lines 39-45: transfer (initialize) with configuration

       (encryption) information)

   b) attempting to communicate with a conditional access management system to

       retrieve active encryption information for a conditional access system; (see

       Addington col. 43, lines 15-30: command processing, conditional access system)

   e) encrypting the content with the default encryption information; (see Addington

       col. 42, lines 52-60: encrypt content with encryption keys) and

   f) distributing the content encrypted with the default encryption information. (see

Addington col. 13, line 46 - col. 14, line 7: content (encrypted) distributed over

communications medium)

Addington does not specifically disclose whereby if communication cannot be

established between the conditional access management system and the

conditional access system.

However, Bestler discloses wherein:

if communication cannot be established between the conditional access

management system and the conditional access system:

d) reading the default encryption information from the default configuration

   memory; (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39;

   col. 5, lines 60-63: encryption information (default) utilized for decryption

   during communications failure)

It would have been obvious to one of ordinary skill in the art to modify

Addington as taught by Bestler to enable the capability for reading the default

encryption information if communication cannot be established.   One of ordinary

skill in the art would have been motivated to employ the teachings of Bestler in

order to enable the capability for a novel and improved method to operate a pay

television (cable system) and permit a subscriber to self-authorize his equipment

to unscramble pay per view programs.   (see Bestler col. 1, lines 28-32)

Regarding Claim 24, Addington discloses the method of claim 23, further comprising:

if communication is achieved between the conditional access management system

and the conditional access system:

b) receiving active encryption information for the content for distribution in the

conditional access system; (see Addington col. 43, lines 2-7; col. 49, lines 58-62;

col. 53, lines 39-45: receive (transfer) encryption keys, normal operation)

c) encrypting the content with the active encryption information; (see Addington col.

42, lines 52-60: content encrypted with encryption keys) and

d) distributing the content encrypted with active encryption information. (see

Addington (see Addington col. 13, line 46 - col. 14, line 7: content (encrypted)

distributed over communications medium)

Regarding Claims 29, 35, Addington discloses a method of default encryption of

content for distribution, comprising:

a) initializing a default configuration memory with default encryption information;

(see Addington col. 12, lines 2-5; col. 45, lines 39-41: configuration (encryption)

information stored in memory)

b) communicating with a conditional access management system to retrieve active

encryption information for the content for distribution in a conditional access

system; (see Addington col. 43, lines 2-7; col. 49, lines 58-62; col. 53, lines 39-

45: transfer configuration (encryption) information)

c) encrypting the content with the active encryption information; distributing the

content encrypted with active encryption information; (see Addington col. 42,

lines 52-60; col. 13, line 46 - col. 14, line 7: content (encrypted) and distributed)

d) signaling all set-top boxes within the conditional access system instructing them

to use the active encryption information; (see Addington col. 43, lines 15-30:

command process, conditional access system; encryption keys sent to set top

box)

f) encrypting the content with the default encryption information; (see Addington

col. 42, lines 52-60: content encrypted with default encryption keys)

g) signaling all set-top boxes within the conditional access system instructing

them to use the default encryption information; (see Addington col. 43, lines

15-30: command processing, conditional access system; col. 43, lines 15-30;

col. 45, lines 25-28: no communications for some set-top boxes, still

connected set top boxes configure using encryption keys) and

h) distributing the content encrypted with the default encryption information. (see

Addington col. 13, line 46 - col. 14, line 7: distributed content for usage by

both connected set-top boxes and disconnected set-top boxes)

Addington does not specifically disclose whereby if a communication failure

occurs between the conditional access management system and the conditional

access system.

However, Bestler discloses wherein:

if a communication failure occurs between the conditional access management

system and the conditional access system:

e) reading the default encryption information from the default configuration

memory; (see Bestler col. 3, lines 1-6; col. 5, lines 19-22; col. 5, lines 37-39;

col. 5, lines 60-63: encryption information (default) utilized for decryption

during communications failure)

It would have been obvious to one of ordinary skill in the art to modify

Addington as taught by Bestler to enable the capability for reading the default

encryption information if communication cannot be established.   One of ordinary

skill in the art would have been motivated to employ the teachings of Bestler in

order to enable the capability for a novel and improved method to operate a pay

television (cable system) and permit a subscriber to self-authorize his equipment

to unscramble pay per view programs.   (see Bestler col. 1, lines 28-32)

Regarding Claims 30, 36, Addington discloses the method of claims 29, 35, further

comprising:

if communication is restored/achieved between the conditional access management

system and the conditional access system:

a) receiving active encryption information for the content for distribution in the

conditional access system; (see Addington col. 43, lines 2-7; col. 49, lines 58-62;

col. 53, lines 39-45: encryption information transferred, normal operation)

b) encrypting the content with the active encryption information; (see Addington col.

42, lines 52-60: content encrypted with encryption keys)

c) signaling all set-top boxes within the conditional access system instructing them

to use the active encryption information; (see Addington col. 43, lines 15-30:

command processing by conditional access system; col. 43, lines 2-7; col. 49,

lines 58-62; col. 53, lines 39-45: configure encryption information) and

d) distributing the content encrypted with active encryption information. (see

Addington col. 13, line 46 - col. 14, line 7: distribute encrypted content)

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another
filed in the United States before the invention by the applicant for patent or (2) a patent granted on an
application for patent by another filed in the United States before the invention by the applicant for patent,
except that an international application filed under the treaty defined in section 351(a) shall have the effects
for purposes of this subsection of an application filed in the United States only if the international
application designated the United States and was published under Article 21(2) of such treaty in the
English language.

6.   Claim **41 - 57** are rejected under 35 U.S.C. 102(e) as being anticipated by

Addington et al. (US Patent No. **7,194,756**).

Regarding Claim 41, Addington discloses an apparatus for default decryption of

content, comprising:

a) a conditional access system; (see Addington Figure 8, number 27 ; col. 12 , lines

22-29: access system for management of cable functions, conditional access

(CA) module (conditional access system)) and

b) a configuration memory capable of storing default decryption information for the

content for use to decrypt the content when the conditional access system

receives signaling instructing it to use the default decryption information. (see

Addington col. 43, lines 15-30: command processing, conditional access system;

col. 12, lines 2-5; col. 45, lines 39-41: memory, storage configuration information)

Regarding Claims 42, 48, 54, Addington discloses the apparatus of claims 41, 47, 52,

wherein the default decryption information comprises default decryption keys. (see

Addington col. 43, lines 2-7; col. 49, lines 58-62; col. 53, lines 39-45:

encryption/decryption information (keys) for content encryption)

Regarding Claims 43, 49, 55, Addington discloses the apparatus of claims 42, 48, 54,

wherein the default decryption keys are unique for each of a plurality of channels. (see

Addington col. 2, lines 60-64: encryption/decryption key unique for each channel)

Regarding Claim 44, Addington discloses the apparatus of claim 41, wherein, when

signaled to initialize the configuration memory, the conditional access system initializes

the configuration memory with default encryption information received with the

signaling. (see Addington col. 43, lines 15-30; col. 45, lines 25-28; col. 45, lines 39-41:

configuration information processed)

Regarding Claims 45, 50, 56, Addington discloses the apparatus of claims 41, 47, 52,

wherein the configuration memory comprises a non-volatile memory. (see Addington

col. 12, lines 2-5: non-volatile memory utilized for operational (configuration)

information)

Regarding Claim 46, Addington discloses the apparatus of claim 41, wherein the

content is decrypted with the default decryption information upon reception of signaling

instructing the conditional access system to use the default decryption information. (see

Addington col. 49, lines 58-62; col. 53, lines 39-45: communication restored, process

configuration (encryption) information)

Regarding Claim 47, Addington discloses an apparatus for default decryption of

content, comprising:

a) means for receiving content in a conditional access system; (see Addington col.

12, lines 22-29: received (encrypted) content; col. 11, lines 57-61; col. 12, lines

2-5: software implementation, means)

b) means for receiving signaling in the conditional access system; (see Addington

col. 12, lines 22-29; col. 15, lines 14-22: conditional access system; col. 43, lines

15-30: command processing; signaling for conditional access system; col. 11,

lines 57-61; col. 12, lines 2-5: software implementation, means)

c) means for storing default decryption information for content received in the

conditional access system for use to decrypt the content when the conditional

access system receives signaling instructing it to use the default decryption

information; (see Addington col. 12, lines 2-5; col. 43, lines 15-30; col. 45, lines

39-41: storage configuration information in memory; col. 11, lines 57-61; col. 12,

lines 2-5: software implementation, means) and

d) means for configuring the storing means with the default decryption information.

(see Addington col. 43, lines 15-30; col. 45, lines 25-28:configure encryption

information; col. 11, lines 57-61; col. 12, lines 2-5: software implementation,

means)

Regarding Claim 51, Addington discloses the apparatus of claim 47, wherein the

content is decrypted with the default decryption information upon reception of signaling

instructing the conditional access system to use the default decryption information. (see

Addington col. 43, lines 15-30: command processing, conditional access system; col.

45, lines 25-28: utilize configuration information, encryption keys)

Regarding Claim 52, Addington discloses a method of default decryption of content,

comprising:

a) receiving signaling instructing storage of default decryption information for

content in a conditional access system; (see Addington col. 45, lines 15-30:

command processing, conditional access system)

b) receiving default decryption information for use to decrypt the content when the

conditional access system receives signaling instructing it to use the default

decryption information; (see Addington col. 43, lines 15-30: command

processing, conditional access system; col. 49, lines 58-62; col. 53, lines 39-45:

receive configuration information)

c) initializing a default configuration memory with the default decryption information;

(see Addington col. 12, lines 2-5; col. 45, lines 39-41: memory, initialized

(storage) configuration information)

d) receiving active decryption information with content in the conditional access

system; (see Addington col. 43, lines 15-30; col. 45, lines 25-28: receive

configuration information)

e) decrypting selected channels with the active decryption information; (see

Addington col. 12, lines 22-29: decrypt content)

if signaling reception instructs use of the default decryption information for the

conditional access system:

f) reading the default decryption information for the content from the default

configuration memory; (see Addington col. 43, lines 15-30; col. 45, lines 25-28:

configure encryption information, normal operation) and

g) decrypting content with the default decryption information. (see Addington col.

12, lines 22-29: decrypt content)

Regarding Claim 53, Addington discloses the method of claim 52, further comprising: if

signaling reception instructs use of active decryption information:

a) receiving active decryption information with the content in the conditional access

system; (see Addington col. 43, lines 15-30; col. 49, lines 58-62; col. 53, lines 39-

45: receive configuration information)

b) decrypting content with the active decryption information. (see Addington col. 12,

lines 22-29: decrypt content)

Regarding Claim 57, Addington discloses a computer readable medium storing

instructions which, when executed on a programmed processor, carry out the process

according to claim 52. (see Addington col. 11, lines 57-61; col. 12, lines 2-5: software

implementation)

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carlton V. Johnson whose telephone number is 571-

270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 -

5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

CVJ
September 4, 2007